United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, March 27, 2012

IT SUPPLY CHAIN

Additional Efforts Needed by National Security-Related Agencies to Address Risks

Statement of Gregory C. Wilshusen, Director
Information Security Issues

March 27, 2012

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-579T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Energy and Commerce, House of Representatives

IT SUPPLY CHAIN

Additional Efforts Needed by National Security-Related Agencies to Address Risks

Why GAO Did This Study

Information technology (IT) systems and the products and services that support them are essential to the operations of the federal government. These products and services are delivered through a complex global supply chain, and the exploitation of vulnerabilities in the IT supply chain is an emerging threat. Federal law requires establishment of information security programs, and implementing standards and guidelines provide for managing supply chain risk.

GAO was asked to testify on its recently issued report that, among other things, identified key risks associated with the supply chains used by federal agencies to procure IT equipment, software, and services, and assessed the extent to which four national security-related agencies have addressed such risks. In producing that report, GAO analyzed federal acquisition and information security laws, regulations, standards, and guidelines; examined departmental policies and procedures; and interviewed officials from four national security-related departments, the intelligence community, and nonfederal entities.

What GAO Recommends

In its report, GAO recommended that the Departments of Energy, Homeland Security, and Justice take steps, as needed, to develop and document policies, procedures, and monitoring capabilities that address IT supply chain risk. In commenting on a draft of the report, the departments generally concurred with the recommendations.

What GAO Found

Reliance on a global supply chain introduces multiple risks to federal information systems and underscores the importance of threat assessments and mitigation. Supply chain threats are present at various phases of a system's development life cycle and could create an unacceptable risk to federal agencies. Key supply chain-related threats include

- installation of intentionally harmful hardware or software (i.e., containing "malicious logic");
- installation of counterfeit hardware or software;
- failure or disruption in the production or distribution of critical products;
- reliance on malicious or unqualified service providers for the performance of technical services; and
- installation of hardware or software containing unintentional vulnerabilities, such as defective code.

These threats can have a range of impacts, including allowing attackers to take control of systems or decreasing the availability of critical materials needed to develop systems. These threats can be introduced by exploiting vulnerabilities that could exist at multiple points in the supply chain. Examples of such vulnerabilities include acquisition of products or parts from unauthorized distributors; application of untested updates and software patches; acquisition of equipment, software, or services from suppliers without knowledge of their past performance or corporate structure; and use of insecure delivery or storage mechanisms. These vulnerabilities could by exploited by malicious actors, leading to the loss of the confidentiality, integrity, or availability of federal systems and the information they contain.

The four national security-related agencies in GAO's review—the Departments of Energy, Homeland Security, Justice, and Defense—varied in the extent to which they have addressed supply chain risks. Specifically, Energy and Homeland Security had not yet defined supply chain protection measures for department information systems and are not in a position to develop implementing procedures and monitoring capabilities. Justice has defined supply chain protection measures but has not developed implementation procedures or monitoring capabilities. Until these agencies develop comprehensive policies, procedures, and monitoring capabilities, increased risk exists that they will be vulnerable to IT supply chain threats. By contrast, the Department of Defense has made greater progress: it has defined supply chain protection measures and implementing procedures and initiated efforts to monitor compliance and effectiveness. In addition, various interagency efforts are under way to address supply chain risks affecting federal IT.

View GAO-12-579T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee:

Thank you for the opportunity to testify at today's hearing on federal and industry efforts related to information technology (IT) supply chain security. As you know, information systems and the products and services that support them are essential for government operations. Federal agencies rely extensively on computerized information systems and electronic data to carry out their operations, and securing these systems and data is essential to protecting national and economic security.

As commerce has become more globalized, the supply chain for IT and services has become increasingly complex.[1] This complexity, in turn, creates potential vulnerabilities that can be exploited by cyber threats, potentially degrading the confidentiality, integrity, and availability of critical and sensitive networks, IT-enabled equipment, and data. These threats can be introduced in the manufacturing, assembly, and distribution of hardware, software, and services and can appear at each phase of the IT system development life cycle. In January 2012, the Director of National Intelligence identified the vulnerabilities associated with the IT supply chain for the nation's networks as one of the greatest strategic cyber threat challenges the country faces.[2] In addition, we have identified the protection of federal information systems as a governmentwide high-risk area since 1997.[3]

My testimony today summarizes the contents of our recently issued report on IT supply chain risks, which, among other things, identified key risks associated with the supply chains used by federal agencies to procure IT equipment, software, or services, and assessed the extent to which four

[1]The National Institute of Standards and Technology (NIST) has defined the term "supply chain" to mean a set of organizations, people, activities, information, and resources for creating and moving a product or service from suppliers through to an organization's customers. Also, NIST defines "information technology" as any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. This includes, among other things, computers, software, firmware, and services (including support services).

[2]Director of National Intelligence, "Worldwide Threat Assessment of the US Intelligence Community," unclassified statement for the record before the Senate Select Committee on Intelligence (Washington, D.C.: Jan. 31, 2012).

[3]See, most recently, GAO, *High-Risk Series: An Update*, GAO-11-278 (Washington, D.C.: February 2011).

national security-related agencies have addressed such risks.[4] In preparing this statement in March 2012, we relied on the work supporting this report. In producing that report, we analyzed federal acquisition and information security laws, regulations, standards, and guidelines; examined departmental policies and procedures; and interviewed officials from four national security-related departments, the intelligence community, and nonfederal entities. The report contains a more detailed overview of the scope of our review and the methodology used. The work on upon which this statement is based was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform audits to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions. We believe that the evidence obtained provided a reasonable basis for our findings and conclusions based on our audit objectives.

Background

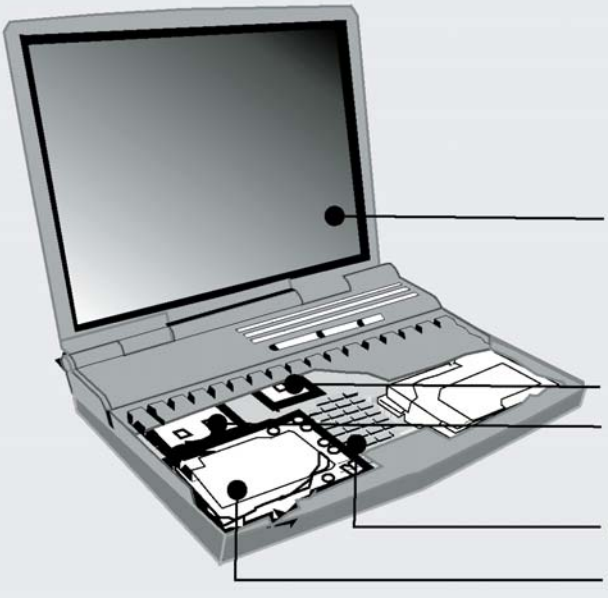
Information systems can be complex undertakings consisting of a multitude of pieces of equipment and software products, and service providers. Each of these components may rely on one or more supply chains. Obtaining a full understanding of the sources of a given information system can also be extremely complex. According to the Software Engineering Institute, the identity of each product or service provider may not be visible to others in the supply chain. Typically, an acquirer, such as a federal agency, will only know about the participants directly connected to it in the supply chain. In addition, the complexity of corporate structures, in which a parent company (or its subsidiaries) may own or control companies that conduct business under different names in multiple countries, presents additional challenges to fully understanding the sources of an information system. As a result, the acquirer will have little visibility into the supply chains of its suppliers.

Federal procurement law and policies promote the acquisition of commercial products when they meet the government's needs. Commercial providers of IT use a global supply chain to design, develop, manufacture, and distribute hardware and software products throughout the world. Many of the manufacturing inputs required for those products—whether physical materials or knowledge—are acquired from various

[4]GAO, *IT Supply Chain: National Security-Related Agencies Need to Better Address Risks*, GAO-12-361 (Washington, D.C.: Mar. 23, 2012).

sources around the globe. Figure 1 depicts the potential countries of origin of common suppliers of various components within a commercially available laptop computer.

Figure 1: Potential Origins of Common Suppliers of Laptop Components



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Source: GAO analysis of public information.

Federal Law Requires Establishment of Information Security Programs, and Implementing Standards and Guidelines Provide for Managing Supply Chain Risk

The Federal Information Security Management Act of 2002 (FISMA) establishes federal agency information security program requirements that support the effectiveness of information security controls over

information resources that support federal operations and assets.[5] Its framework creates a cycle of risk management activities necessary for an effective security program, and it assigns responsibilities to the National Institute of Standards and Technology (NIST) for providing standards and guidelines on information security.[6]

In its August 2009 revision of Special Publication (SP) 800-53 (Revision 3), which provides recommended security controls for federal agencies and organizations,[7] NIST included for the first time a security control for supply chain protection (SA-12).[8] SA-12 identified several specific measures organizations could use to provide additional supply chain protections, such as conducting due diligence reviews of suppliers; using trusted shipping and warehousing; and employing independent analysis and penetration testing of IT systems, components, and products. In addition, SP 800-53, Revision 3, includes a security control for system and service acquisition policies and procedures (SA-1).[9] Thus, for systems where both controls are selected, agencies should develop, disseminate, and review acquisition policy and implementing procedures that help protect against supply chain threats throughout the system development life cycle.[10] Further, in March 2011, NIST published SP 800-

[5]Title III of the E-Government Act of 2002, Pub. L. No. 107-347, Dec. 17, 2002.

[6]FISMA requires that federal agencies comply with NIST information security standards, and agencies may not waive their use. In addition, FISMA requires agencies to develop, document, and implement agencywide programs to provide security for the information systems that support their operations and assets.

[7]NIST, *Recommended Security Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 3 (Gaithersburg, Md.: May 2010).

[8]SA-12 states that an organization should define and employ a list of measures to protect against supply chain threats as part of a comprehensive, defense-in-breadth information security strategy. According to SP 800-53, Revision 3, SA-12 should be selected for the initial control baseline of all agency information systems categorized as high impact.

[9]SA-1 states that organizations should develop formal, documented procedures to facilitate the implementation of system and services acquisition policy and associated system and services acquisition family of controls, which includes SA-12. According to SP 800-53, Revision 3, SA-1 should be selected for the initial control baseline regardless of categorization.

[10]These controls are required for both non-national security and national security systems. Specifically, OMB requires federal agencies to use SP 800-53 for selecting controls for non-national security systems, while the Committee on National Security Systems, a committee established to issue policy directives and instructions on information security for national security systems, has established SP 800-53 as a common foundation for information security controls for national security systems.

39, an approach to organizationwide management of information security risk, which states that organizations should monitor risk on an ongoing basis as part of a comprehensive risk management program.[11]

IT Supply Chain Presents Numerous Information Security Risks to Federal Agencies

Reliance on a global supply chain introduces multiple risks to federal information systems and underscores the importance of threat assessments and risk mitigation. Supply chain threats are present at various phases of a system's development life cycle. Key threats that could create an unacceptable risk to federal agencies include the following:

- installation of hardware or software containing malicious logic, which is hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose;
- installation of counterfeit hardware or software, which is hardware or software containing non-genuine component parts or code;
- failure or disruption in the production or distribution of critical products resulting from manmade or natural causes;
- reliance on a malicious or unqualified service provider for the performance of technical services; and
- installation of hardware or software that contains unintentional vulnerabilities, such as defects in code that can be exploited.

Such threats can have a range of impacts, including allowing attackers to take control of systems and read, modify, or delete sensitive information; decreasing the reliability of IT equipment; decreasing the availability of material needed to develop systems; or allowing remote attackers to cause a denial of service, among other things.

Threat actors can introduce these threats into federal information systems by exploiting vulnerabilities that could exist at multiple points in the global supply chain. In addition, supply chain vulnerabilities can include weaknesses in agency acquisition or security procedures, controls, or implementation related to an information system. Examples of types of vulnerabilities that could be exploited include

[11]NIST, *Managing Information Security Risk: Organization, Mission, and Information System View*, SP 800-39 (Gaithersburg, Md.: March 2011).

- acquisition of IT products or parts from sources other than the original manufacturer or authorized reseller, such as independent distributors, brokers, or on the gray market;
- applying untested updates and software patches to information system components;
- acquiring equipment, software, or services from suppliers without understanding their past performance or corporate structure; and
- using delivery or storage mechanisms that are not secure.

If a threat actor exploits an existing vulnerability, it could lead to the loss of the confidentiality, integrity, or availability of the system and associated information.

Three National Security-Related Agencies Have Not Fully Addressed IT Supply Chain Risk

Although the four agencies in our review—the Departments of Energy, Homeland Security (DHS), Justice, and Defense—have acknowledged the risks presented by supply chain vulnerabilities, they varied in the extent to which they have addressed these risks by (1) defining supply chain protection measures for department information systems, (2) developing implementing procedures for these measures, and (3) establishing capabilities for monitoring compliance with and the effectiveness of such measures.

Three of the four departments have made limited progress in addressing supply chain risk:

- In May 2011, the Department of Energy revised its information security program, which requires Energy components to implement provisions based on NIST and Committee on National Security Systems guidance. However, the department was unable to provide details on implementation progress, milestones for completion, or how supply chain protection measures would be defined. Because it had not defined these measures or associated implementing procedures, the department was also not in a position to monitor compliance or effectiveness.
- Although its information security guidance mentions the NIST control related to supply chain protection, DHS has not defined the supply chain protection measures that system owners should employ. The department's information security policy manager stated that it was in the process of developing policy that would address supply chain protection, but did not provide details on when it would be completed. In addition, in the absence of such a policy, DHS was not in a position

to develop implementation procedures or to monitor compliance or effectiveness.

- The Department of Justice has defined specific security measures for protecting against supply chain threats through the use of provisions in vendor contracts and agreements. Officials identified (1) a citizenship and residency requirement and (2) a national security risk questionnaire as two provisions that address supply chain risk. However, Justice has not developed procedures for ensuring the effective implementation of these protection measures or a mechanism for verifying compliance with and the effectiveness of these measures.

By contrast, the Department of Defense has made more progress. Specifically, the department's supply chain risk management efforts began in 2003 and include

- a policy requiring supply chain risk to be addressed early and across a system's entire life cycle and calling for an incremental implementation of supply chain risk management through a series of pilot projects;
- a requirement that every acquisition program submit and update a "program protection plan" that is to, among other things, help manage risks from supply chain exploits or design vulnerabilities;
- procedures for implementing supply chain protection measures, such as an implementation guide describing 32 specific measures for enhancing supply chain protection and procedures for program protection plans identifying ways in which programs should manage supply chain risk; and
- a monitoring mechanism to determine the status and effectiveness of supply chain protection pilot projects, as well as monitoring compliance with and effectiveness of program protection policies and procedures for several acquisition programs.

In addition, the four national security-related agencies participate in interagency efforts to address supply chain security, including participation in the Comprehensive National Cybersecurity Initiative,[12] development of technical and policy tools, and collaboration with the intelligence community. In support of the cybersecurity initiative, Defense

[12]Begun by the Bush administration in 2008, the Comprehensive National Cybersecurity Initiative is a series of initiatives aimed at improving cybersecurity within the federal government. This initiative, which is composed of 12 projects with the objective of safeguarding federal executive branch information systems, includes a project focused on addressing global supply chain risk management.

and DHS jointly lead an interagency initiative on supply chain risk management to address issues of globalization affecting the federal government's IT. Also, DHS has developed a comprehensive portfolio of technical and policy-based product offerings for federal civilian departments and agencies, including technical assessment capabilities, acquisition support, and incident response capabilities. Further, the four national security-related departments participate in an Office of the National Counterintelligence Executive-led initiative to (1) develop a common methodology for conducting threat assessments on entities that do business with the national security community and (2) request from agencies and centrally store copies of threat assessments for future use by components of the national security community.

Three National Security-Related Departments Need to Take Action to Better Address IT Supply Chain Risks

To assist the three national security-related agencies in better addressing IT supply chain-related security risks for their departmental information systems, we made several recommendations to the Secretaries of Energy and Homeland Security and the Attorney General. Specifically, we recommended that Energy

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

In commenting on our report, Energy stated that it concurred with the spirit of our recommendations. Energy also expressed concern that the recommendations are not fully aligned with the administration's initiatives and stated that it believes policies and standards to address IT supply chain risk management must be coordinated at the national level, not independently through individual agencies. We agree that national or federal policies and standards should be coordinated and promulgated at the national or federal level. However, we also believe–as intended by our recommendations—that federal departments are responsible for developing departmental policies and procedures that are consistent and aligned with federal guidance. Our recommendations to Energy are based

on and consistent with federal guidance on supply chain risk management.

In addition, we recommended that DHS

- develop and document departmental policy that defines which security measures should be employed to protect against supply chain threats;
- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

In commenting on a draft of our report, DHS concurred with our recommendations and described steps the department is taking to address them, including developing departmental policy to define supply chain protection measures, examining risk management procedures, and exploring options for verifying compliance with and effectiveness of its supply chain protection measures.

We also recommended that Justice

- develop, document, and disseminate procedures to implement the supply chain protection security measures defined in departmental policy; and
- develop and implement a monitoring capability to verify compliance with, and assess the effectiveness of, supply chain protection measures.

Justice concurred with the recommendations.

In summary, the global IT supply chain introduces a myriad of security vulnerabilities to federal information systems that, if exploited, could introduce threats to the confidentiality, integrity, and availability of federal information systems. Thus the potential exists for serious adverse impact on an agency's operations, assets, and employees. These risks highlight the importance of national security-related agencies fully addressing supply chain security by defining measures and implementation procedures for supply chain protection and monitoring compliance with and the effectiveness of these measures. Until these agencies develop comprehensive policies, procedures, and monitoring capabilities, increased risk exists that they will be vulnerable to IT supply chain threats.

Chairman Stearns, Ranking Member DeGette, and Members of the Subcommittee, this completes my statement. I would be happy to answer any questions you have at this time.

Contact and Acknowledgments

If you have any questions regarding this statement, please contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov. Other key contributors to this statement include Michael W. Gilmore (Assistant Director), Bradley W. Becker, Kush K. Malhotra, and Lee McCracken.